非可換群を用いた完全準同型暗号の構成および関連する問題*

産業技術総合研究所
縫田 光司 (k.nuida@aist.go.jp)

平成 27 年 4 月 8 日

1 公開鍵暗号

A さんが離れた場所にいる B さんに秘密の情報（「平文」）m を送る状況を考えます。そのための数学的な仕組みとして、まず A さんが「暗号化」アルゴリズムで m を「暗号文」$c = \mathsf{Enc}(m)$ へと変換して c を B さんに送り、B さんは受け取った暗号文 c を「復号」アルゴリズムでもとの平文 $m = \mathsf{Dec}(c)$ に戻す、という暗号化通信技術があります。こうすると、途中の通信を悪い人（「攻撃者」）に盗み見られたとき、見られるのは m 自体ではなく変換後の暗号文 c なので、素朴に考えると通信の安全性が増していると期待されます。ただし、攻撃者が復号アルゴリズム Dec を知っている状況では、攻撃者が盗み見た暗号文 c から自力で平文 m を復元できてしまうため、全く安全ではありません。これを避けるため、復号アルゴリズムは第三者に対して秘密にする必要があります。実用上は、復号アルゴリズムの入力として暗号文以外に「復号鍵」という補助情報を用いることで、たとえアルゴリズムが攻撃者に知られても、復号鍵さえ秘密に保たれていれば安全性が損なわれないように設計します。また、この変更の影響で、暗号化アルゴリズムも、復号鍵に対応する「暗号化鍵」を補助入力として用いることになります。

暗号化技術のうち、暗号化鍵と復号鍵が異なり、さらに暗号化鍵から対となる復号鍵を容易に特定できない性質を持つものを「公開鍵暗号」といいます。このとき、復号鍵だけを B さん（受信者）が秘密に保持しておけば（この復号鍵を「秘密鍵」といいます）、暗号化鍵は誰に公開しても安全性が損なわれないため（この暗号化鍵を「公開鍵」といいます）、同じ秘密鍵を用いて世界中の誰とでも暗号化通信が可能となります。

例 1. ElGamal 暗号 [1] という公開鍵暗号方式では、有限巡回群 G とその生成元 g、およびある（ランダムな）整数 s を用いて $h = g^s$ で定められる元 h

*この文章は、2014 年 5 月 15 日に室蘭工業大学談話会で発表した内容に基づくものです。

の三つ組 (G, g, h) を公開鍵、h の計算に用いた s を秘密鍵とします。平文 m は群 G の元であるとし、暗号化アルゴリズムを $\mathsf{Enc}(m) = (g^r, h^r m) \in G \times G$（ただし r はランダムな整数）、復号アルゴリズムを $\mathsf{Dec}(c) = {c_1}^{-s} c_2$（$c = (c_1, c_2) \in G \times G$）で定義します。このとき、（暗号化に用いた r が何であっても）$\mathsf{Dec}(\mathsf{Enc}(m)) = m$ が成り立ち、通信を正しく実行できます。なお、この暗号化方式が安全かどうかは群 G の具体的な構成方法に依存します。

2　準同型暗号とその応用

公開鍵暗号方式の平文の全体集合 $\mathcal{M}$ 上に（一つもしくは複数の）「基本演算」op が定義されている状況を考えます。さらに、暗号文の全体集合 $\mathcal{C}$ 上に、基本演算 op（例えば n 項演算とします）の各々に対応する「準同型演算」$\overline{\mathsf{op}}$ が定義されているとします。これらの演算が、あらゆる $m_1, \ldots, m_n \in \mathcal{M}$ について、（微小な確率を除き）

$$\mathsf{Dec}(\overline{\mathsf{op}}(\mathsf{Enc}(m_1), \ldots, \mathsf{Enc}(m_n))) = \mathsf{op}(m_1, \ldots, m_n) \tag{1}$$

を満たすとき、この暗号方式を「準同型暗号」といいます。

例 2. 上述した ElGamal 暗号について、$\mathsf{op}(m, m') := m \cdot m'$（$m, m' \in \mathcal{M} = G$）、$\overline{\mathsf{op}}(c, c') := c \cdot c'$（$c, c' \in \mathcal{C} = G \times G$）と演算を定義すると、条件 (1) が成り立ち、ElGamal 暗号は準同型暗号となります。（平文の演算が群の乗法であることを強調したいときは「乗法準同型暗号」ともいいます。）

一方、平文の全体集合が加法群であるような準同型暗号（「加法準同型暗号」ともいいます）の例としては Paillier 暗号 [2] などがあります。Paillier 暗号では、同程度の大きさの異なる素数 p, q について $N := pq$ で定まる法に関する整数剰余群 $\mathbb{Z}/N\mathbb{Z}$ が平文の全体集合となります。なお、この暗号化方式が安全であるためには、N の素因数分解の計算が充分な難しさを持つように p と q を大きく選ぶ必要があります。

これらの準同型暗号の機能は、「暗号化した状態のままで平文に対する掛け算や足し算を計算できる」とも言えます。こうした「平文を見ずに平文の演算を行える」機能ゆえ、準同型暗号は、電子投票（個々人の投票先を秘密にしたまま当選者を決定したい）や、いわゆるビッグデータ解析におけるプライバシー保護（個々の個人データの詳細を秘密にしたまま全体の統計情報のみを得たい）といった様々な分野への応用が期待されています。話者の勤務先でもそうした応用の研究を行っています。詳しくは [3, 4] をご覧ください。

3　話者の研究：非可換群を用いた完全準同型暗号

上述した準同型暗号の例である ElGamal 暗号や Paillier 暗号は、それぞれ平文に対する乗法（群演算）や加法といった単一の演算にしか対応していま

せん。一方、比較的最近の研究 [5] により、平文の全体集合 $\mathcal{M} := \mathbb{F}_2$ における加法と乗法の両方に対応した準同型暗号方式が実現されました。$\mathbb{F}_2$ に値をとる $\mathbb{F}_2$ 上の（多変数）関数はすべて $\mathbb{F}_2$ 係数多項式として表せるため、上記 2 種類の準同型演算の組み合わせにより、平文に対するあらゆる演算を暗号化したままで行うことが可能です。このような、平文のあらゆる演算に対応した準同型暗号は「完全準同型暗号」と呼ばれます。

完全準同型暗号については、これまでにより効率的なアルゴリズムの構成や平文の全体集合の拡張など多くの研究が行われていますが、1 ビット平文の場合（$\mathcal{M} = \mathbb{F}_2$）でさえ、本稿執筆時点では（最初の方式 [5] よりかなり改善されたとはいえ）計算速度などの効率が悪いため大規模な応用に適するとは言い難い状況です。こうした既存方式では、基盤となる数理構造として多項式環の剰余環や整数剰余環などの可換な構造が利用されていますが、話者の最近の研究 [6] では、非可換群を利用した新たな完全準同型暗号の構成原理を模索しています。その肝となるのが以下の事実です。

命題 1. 有限体 $\mathbb{F}_q$ 上の 2 次特殊線型群 $G = \mathrm{SL}_2(\mathbb{F}_q)$ について、$X := G \backslash \{\pm I\}$ と定める。このとき、$x, y \in X$ に対して、$r \in G$ を一様ランダムに選ぶとき、

$$\Pr[\ [x,y]_r \notin X\ ] = O(q^{-1}) \tag{2}$$

が成り立つ。ここで $[x,y]_r$ は

$$[x,y]_r := [rxr^{-1}, y] = (rxr^{-1}) \cdot y \cdot (rxr^{-1})^{-1} \cdot y^{-1} \tag{3}$$

で定義される。

$G := \mathrm{SL}_2(\mathbb{F}_q)$ について、$G \times G$ の部分集合 $\mathcal{C}_0$ と $\mathcal{C}_1$ を

$$\mathcal{C}_0 := \{(x,y) \mid y \in X, x = I\} \tag{4}$$

$$\mathcal{C}_1 := \{(x,y) \mid y \in X, x = y\} \tag{5}$$

で定義します。また、$(x,y), (x',y') \in G \times G$ について

$$\neg(x,y) := (x^{-1}y, y) \tag{6}$$

および

$$(x,y) \wedge (x',y') := ([x,x']_r, [y,y']_r) \tag{7}$$

（ただし $r \in G$ は一様ランダムな元、また $[x,y]_r$ は (3) の通り）と定義します。すると、$b, b' \in \{0,1\}$ について、

$$(x,y) \in \mathcal{C}_b \text{ ならば } \neg(x,y) \in \mathcal{C}_{\neg b} \tag{8}$$

（$\neg b$ はビット b に対する NOT 演算：$\neg b = 1 - b$）および

$$(x,y) \in \mathcal{C}_b, (x',y') \in \mathcal{C}_{b'} \text{ ならば、確率 } O(q^{-1}) \text{ を除き } (x,y) \wedge (x',y') \in \mathcal{C}_{b \wedge b'} \tag{9}$$

($b \wedge b'$ はビット b, b' に対する AND 演算）が命題 1 により成り立ちます。つまり、$\mathcal{C}_b$ の元をビット b と対応付けることで、ビットの NOT 演算と AND 演算が群 $G \times G$ の中で（微小な確率を除いて）計算できることになります。話者の研究では、この機構を用いた完全準同型暗号の構成を目指しています。具体的には、上述した通り上記の機構により NOT 演算と AND 演算を計算できるのですが、目標は NOT 演算と AND 演算を「安全に」計算することであり、この機構を「安全に」実現する方法がまだ見付かっていません。この点が現在の主な研究課題です。

参考文献

[1] T. ElGamal: A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* vol.31, no.4, 1985, pp.469–472

[2] P. Paillier: Public-key cryptosystems based on composite degree residuosity classes. In: *Proceedings of EUROCRYPT 1999*, Lecture Notes in Computer Science vol.1592, Springer, 1999, pp.223–238

[3] 「化合物データベースの秘匿検索技術」、`https://www.youtube.com/watch?v=1J_wiykXArE`

[4] 「スマホで安心「共ダチ探し」　トモサガ」、`https://www.youtube.com/watch?v=NVE1k_DQOXU`

[5] C. Gentry: Fully homomorphic encryption using ideal lattices. In: *Proceedings of STOC 2009*, ACM, 2009, pp.169–178

[6] K. Nuida: A simple framework for noise-free construction of fully homomorphic encryption from a special class of non-commutative groups. Preprint, IACR Cryptology ePrint Archive 2014/097, 2014, `http://eprint.iacr.org/2014/097`